GLOBAL CONNECTIONS

Coalition Partner Sites

CWID 2007 is the premier event to investigate coalition interoperability issues. Coalition partners work with U.S. organizations and agencies to define information technology solutions that can be applied in the real-world environment. CWID warfighters and operators assess utility, information assurance, software or procedural capabilities that address unique requirements in each country.

Directed by the Chairman of the Joint Chiefs of Staff, the annual demonstration conducts interoperability trials to assess new and evolving technologies and capabilities enabling information exchange among government and non-government agencies, Services, combatant commands and multinational participants.

CWID leadership emphasizes concepts of operations and tactics, techniques and procedures that facilitate a more flexible and responsive fielding solution for multinational operations.

U.S. European Command (USEUCOM) is the host combatant command for the second consecutive year. Since USEUCOM is the only combatant command headquartered outside the United States, it provides opportunity for a day-to-day coalition operational environment. USEUCOM is scheduled to host an unprecedented third CWID in 2008.

The event examines a range of technologies to enhance the collaborative information environment the U.S. Joint Chiefs of Staff, U.S. combatant commanders and other defense agencies are developing. Each participating nation brings unique agendas and interoperability objectives to information technologies demonstrated at domestic and coalition sites around the world.

Information sharing over multiple security domains is an architecture challenge CWID meets every year during execution, creating a global network of more than 25 operating locations. The complex coalition community, reflective of real-world operations, is a relationship challenge as well as a technological one. CWID engineers and technology candidates are reaching unprecedented transparency.

CWID continues to redefine "coalition" to include Homeland Security and Homeland Defense (HS/HD) partners, first responders, other government and non-government entities and allied equivalents. The larger community was first embraced in 2004 when U.S. Northern Command (USNORTHCOM) hosted CWID with objectives to support allies in counterterrorism and disaster response.

Hosting CWID at a forward-deployed U.S. combatant commander focuses the event on the forward-deployed warfighter and on the Coalition environment.

U.S. SCHEDULE OF EVENTS

May 29-June 22: Execution

- **May 29-June 1:** National Integration/Final Testing and Trial Set-Up
- **June 4-8:** Coalition Integration, Scenario Training and Rehearsal
- **June 11-15:** Execution and Assessment
- **June 18-21:** Visitor Week
- **June 22:** Hot Wash

PARTICIPANTS

- CANADA
- DENMARK
- FRANCE
- GERMANY
- ITALY
- THE NETHERLANDS
- NEW ZEALAND
- NORWAY
- POLAND
- PORTUGAL
- ROMANIA
- SPAIN
- TURKEY
- UNITED KINGDON
- UNITED STATES
- NATO

OBSERVERS

- AUSTRALIA
- AUSTRIA

NATO OBSERVERS

- CZHECH REPUBLIC
- ESTONIA
- HUNGARY

PARTNERSHIP FOR PEACE PARTICIPANTS

- FINLAND
- SWEDEN

COMBINED COMMUNICATIONS ELECTRONICS BOARD

Developing Solutions for Canada

The Coalition Warrior Interoperability Demonstration provides Canada with a dynamic opportunity to evaluate new and emerging C4I technologies for use in the Canadian Forces and other government departments, and to develop solutions to interoperability challenges nationally, and with Canada's principal allies.

Canada's participation in CWID has been primarily a program of the Department of National Defence (DND) in conjunction with other Allied militaries. Since 2004, Public Safety and Emergency Preparedness Canada (PSEPC) has partnered with DND, mirroring CWID participation of Homeland Security / Defence organizations by the United States. This year's CWID will feature the Government Operations Centre (GOC) taking the lead for the Homeland Security Scenario, working closely with their US counterparts. In addition to GOC, CWID 2007 is once again marked by an increased awareness and support by other government departments and their attendant agencies. This has allowed CWID to evolve into a venue that explores solutions for purely military purposes as well as those of common interest to domestic security and public safety organizations within Canada.

The aim of Canada's participation is to enhance interoperability within a military coalition and domestic security environment.

SUPPORTING TRANSFORMATION

As the Canadian Forces (CF) continues to transform, the current security environment calls for professional, highly-trained

armed forces capable of using new technologies effectively in joint, interagency and multinational operations. New technologies offer fast, flexible solutions to such operational problems as delivering force precisely in a war zone, or monitoring the flow of refugees in a humanitarian crisis. The CF has embraced these new technologies, and will continue to invest in training and equipping Regular and Reserve personnel to ensure they remain amongst the most highly trained, technologically adept soldiers, sailors, air force personnel in the world.

The transformation process is evolutionary and has no definable end state. Transformation focuses on people, technology, ways of conducting operations and ways of thinking. It does not seek to re-structure the CF completely, or re-equip it, but rather to blend

CANADIAN OBJECTIVES

The objectives for Canadian participation in CWID 2007 are:

1. Cross Domain Data Sharing
2. Integrated Intelligence
3. Integrated Operations
4. Integrated Logistics
5. Integrated Planning
6. Integrated Communications

SENIOR NATIONAL REPRESENTATIVE

Col R.J. Chekan
Commandant CFEC

For more information on CWID, visit the following sites:
http://www.cwid.js.mil/
http://www.ops.forces.gc.ca/cfec

NATIONAL CWID 2007 SITES

Canadian participation will involve activities within Canada, NATO, US, UK, and NZ.

- The Canadian Forces Experimentation Centre (CFEC), located at Shirley's Bay, Ottawa Ontario coordinates all experimentation and Interoperability Trials for Canada within the CWID program and will be the main site for CWID 2007.
- Other Canadian sites include Valcartier Quebec, Winnipeg Manitoba, and two technical sites in the Ottawa area.

PARTICIPATION AT COALITION SITES

Canada will deploy staff to the main NATO CWID site in Lillehammer Norway, the Coalition Air Component site at Hanscom AFB Massachusetts, and Coalition Maritime Component site in San Diego California. Canada will host war fighters from the United Kingdom.

CWID ACCREDITATION AND SECURITY ISSUES

Mr. Bill Munro
Network Security Accreditation
613-949-6752
munro.wr@forces.gc.ca

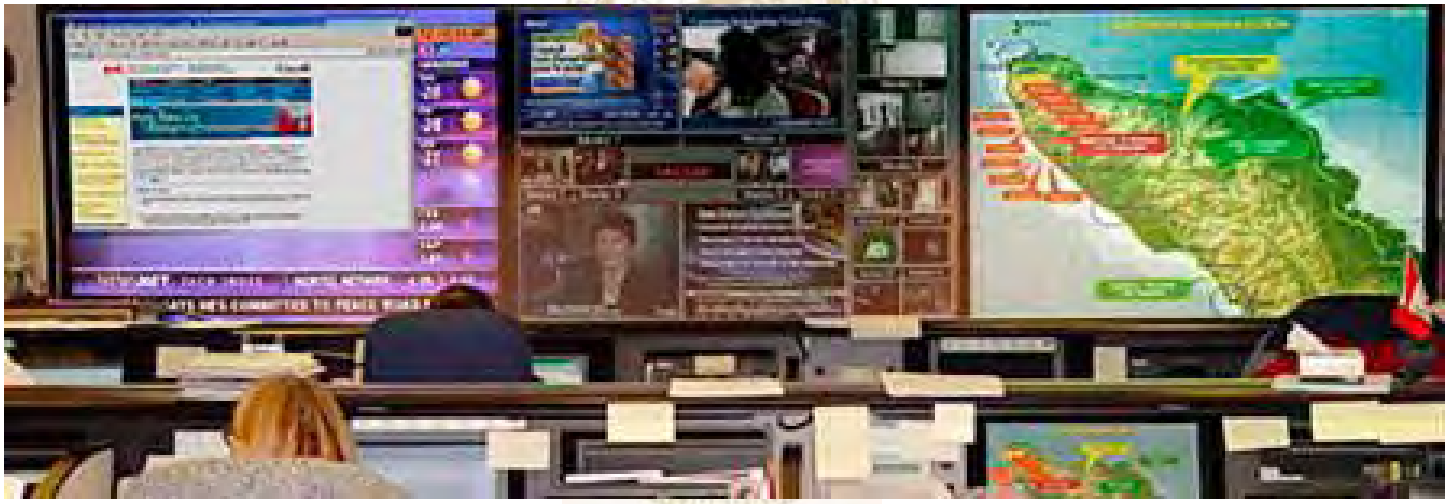
ALL VIPS AND VISITORS TO CF CWID SITES CONTACT

John MacLean, CFEC
613.990.7542
maclean.ji@forces.gc.ca

CANADIAN TRIAL PARTICIPATION

CANADIAN LED TRIALS		DEVELOPER	*TRIALS SECTION PAGE
1.56	Dual Diode (One-Way) Data Transfer System (Dual Diode)	Owl Computing Technologies, Inc.	6
1.61	INREGRITY Secure Workstation (INTSecWS)	Green Hills Software, Inc.	7
2.16	Deployable Geospatial Database (DGDB)	MCE and SimActive	9
2.57	Automatic Image Mosaic and Mapping System (AIMM)	PCI Geomatics	11
3.71	MobiKEY Identity Base Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Route1, Inc.	17
6.15	Geolap	MCE	22
6.36	Joint Network Defence and Management System (JNDMS)	MDA Corp.	23
6.66	IP Interoperability and Collaboration System (IPICS)	Cisco Systems, Inc.	24
CANADIAN PARTICPATION			
3.14	Coalition Secure Management and Operations System (COSMOS)	US OSD, DISA, NSA, CDM	12
3.38	Collaborative Decision Aid (CDA)	ARINC Engineering Services, LLC	15
3.39	Command, Control, Communications, Computers and Intelligence Defense Joint System (C4I Defense)	SELEX-SI SpA	15
3.70	Coalition open Joint Operations Picture (CoJOP)	Fujitsu Services	17
5.59	Mission Planning System (MPS)	Collaboration Technologies, Inc.	20
6.89	Enhanced Video Text and Audio processing (eVITAP)	Virage, Inc.	25

*Some technical detail on all trials listed is contained in the back of this Guidebook at the Trials Tab



existing and emerging systems and structures to create greatly enhanced capabilities relevant to future missions, roles and tasks.

CWID SUPPORTS TRANSFORMATION BY:

- Aiding improved coordination with other government departments and interoperability with allied forces through the investigation of emerging technology
- Providing a venue to explore new solutions for command, control, communications, computers, intelligence, surveillance and reconnaissance capabilities (C4ISR)
- Allowing greater emphasis on the experimentation of technologies that can support developing doctrine, concepts and capabilities
- Hands-on testing of the technologies on trial in a way that closely resembles how they would be used in operations by trained, technologically adept soldiers, sailors, air force personnel

DUAL SCENARIOS

For CWID 2007, two scenarios were created. One scenario involves a traditional military expeditionary coalition in a fictional region overseas. The second scenario addresses the requirements of domestic security within North America. For the military coalition scenario, Canada's focus is on a unified national command and an integrated force involving all three Environmental Elements operating seamlessly with coalition partners. The domestic security scenario is led by PSEPC with close participation from DND, the RCMP and other Government Agencies. The primary international partner for the domestic security scenario is the United States with its various Homeland Security / Defence Agencies.

EXPERIMENT DIRECTOR

Major George Sherwood, CFEC
613.990.7506
sherwood.g2@forces.gc.ca

PUBLIC AFFAIRS OFFICER

John MacLean, CFEC
613.990.7542
maclean.ji@forces.gc.ca

TRIAL COORDINATOR

Mr. Andreas Psarras, CFEC
613.990.7647
psarras.ap@forces.gc.ca

SYSTEM ENGINEER AND NETWORK MANAGER

Mr. Walter Baziuk, CFEC
613.990.7602
baziuk.wg@forces.gc.ca

SCENARIO COORDINATOR

Mr. Paul McCumber, Contractor
613.990.7602
mccumber.pr@forces.gc.ca

OPERATIONAL RESEARCH

Ms. Melanie Bernier, CFEC
613.991.6151
bernier.my@forces.gc.ca

Mr. Krzysztof Skonieczny
613-990-7461
skonieczny.k@forces.gc.ca

POINTS OF CONTACT

AIR FORCE AND NATO AIR FORCE

Maj Walter Norquay, Sponsor
613.990.2539
norquay.wsf@forces.gc.ca

Capt Paul Bolduc
Air Force & National NATO Lead
613.944.5708
bolduc.jvp@forces.gc.ca

Mr. Abder Sahi
Air Force Technical POC
418.844.4000 ext 4455
abderrazak.sahi@drdc.rddc.gc.ca

NAVY

Lt(N) Barrie Wells, 819-997-6568
wells.b@forces.gc.ca

GOVERNMENT OPERATIONS CENTRE

Role of the Government Operations Centre

- To provide strategic level direction and coordination on behalf of the Government of Canada in response to an emerging or occurring event affecting the national interest.

What is the Government Operations Centre (GOC)?

- The GOC is the Government of Canada's strategic level operations centre, providing support to the federal government in five key functional areas: 24/7 monitoring and reporting of events that affect the national interest; developing situational awareness, risk assessment, alerting and warning products; event specific contingency planning; cyber security activities; and response management.

The GOC, while housed within Public Safety and Emergency Preparedness Canada (PSEPC), functions on behalf of the Government of Canada. The trained staffs are interdepartmental and interagency, drawn from PSEPC and our federal partners.

The GOC works at the hub of a network of operations centres run by a variety of federal departments and agencies including

among others, the Royal Canadian Mounted Police, Public Health Agency of Canada, Foreign Affairs, Transport Canada, Canadian Security and Intelligence Service and National Defence in order to manage the national response. The GOC also maintains contact, and works directly with the provinces and territories as well as international partners such as the United States, U.K, Australia, New Zealand, the U.N. and NATO.

As the only strategic level operations centre in Canada, it supports senior level political decision-making (up to Prime Minister), through the analysis of situation data and dissemination of strategic decisions to the operation centres to which it is linked, but that operate at lower, more functional levels. Strategic operations are "whole of government" and include political decision-making that almost always involves co-ordinated interagency, multi-jurisdictional and multinational responses. As required, the GOC provides strategic coordination on behalf of the Government of Canada in reference to matters affecting the national interest within and beyond Canada's borders and coordinates national efforts with similar centres internationally.

CANADIAN FORCES EXPERIMENTATION CENTRE (CFEC)

CFEC PROVIDES THE VENUE AND LEADERSHIP required for successful CWID execution. Primarily CFEC is responsible to:

- Provide military personnel and Defence Scientists at the Canadian Main Site to augment Joint and Tactical Operational Assessment Teams
- Coordinate the National Experimentation Campaign for CWID
- Form and coordinate the Coalition Data Assessment Team
- Coordinate all Interoperability Trial equipment, personnel, assessment, and reports
- Coordinate CFX Net connectivity for Canadian Sites, including Trial Engineer Support, Cryptography, and Network Security Accreditation
- Collect and compile all data to produce a CWID 2007 Final After Action Report
- Produce and distribute the CWID 2007 Executive Summary outlining all National and Coalition achievements and "Lessons Learned" during CWID Execution
- Coordinate VIP visits, Media Day, and Coalition Staff in/out of Canada

Currently, CFEC successfully manages CWID for seven DND organizations (DAR, DMRS, MCE, JIIFC Det, DLCI, Canada Command and NDCC) and 2 Other Government Department's (PSEPC GOC and RCMP). Each organization involved has found the value of using CWID as a test bed to try and fill their capability gaps with new and emerging technologies. This point is effectively demonstrated by PSEPC GOC's growing involvement over the last few years. This year, they are planning to bring a team of six during CWID execution, their biggest team yet.

ARMY
Major David Pichette
613-995-6475
pichette.d@forces.gc.ca

GOC
Anik Bertrand
613-991-7000
anik.bertrand@
psepc-sppcc.gc.ca

Shane Livingstone
613 991-5028
shane.livingstone@
psepc-sppcc.gc.ca

JIIFC DET
Maj Peter Lipohar
613 944-7962
lipohar.p@forces.gc.ca

CANADA COMMAND
LCol Sean Sullivan
613 943-6367
sullivan.ts@forces.gc.ca

COALITION OPERATIONS PARTICIPANTS

- Directorate Intelligence Information Management
- Director Land Command Information
- Directorate Land Requirements
- Directorate Air Programmes
- Directorate Maritime Requirements – Sea
- Joint Information and Intelligence Fusion Capability
- Directorate Information Management Security
- Directorate of Joint Capability Production
- Mapping and Charting Establishment
- Joint Imagery Centre
- Mapping and Charting Establishment
- Information Operations Group

HOMELAND SECURITY PARTICIPANTS

DEPARTMENT OF NATIONAL DEFENCE

- Canada Command
- Chief of Defence Intelligence
- Mapping and Charting Establishment
- Joint Imagery Centre
- Joint Information and Intelligence Fusion Capability
- Directorate of Joint Capability Production
- Director Land Command Information

OTHER GOVERNMENT AGENCIES

- Government Operations Centre
- Royal Canadian Mounted Police





COMBINED COMMUNICATIONS ELECTRONICS BOARD

New Zealand Defence Force

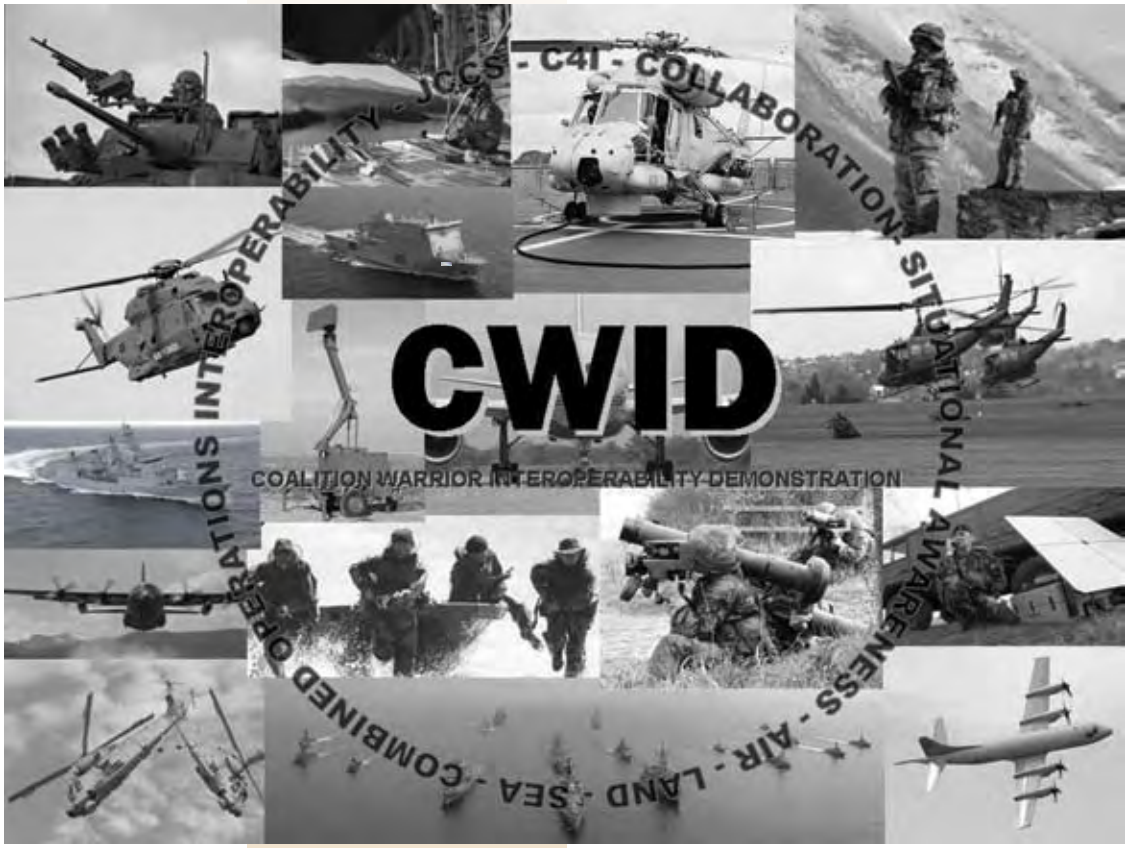
Coalition Warrior Interoperability Demonstration (CWID) provides the New Zealand Defence Force (NZDF) the best means currently available to participate in the collective development, demonstration and assessment for suitability of C4I capability and technology solutions to meet near term interoperability challenges in a joint, coalition and civil authority environment.

AIM

The aim of NZDF participation in CWID is to assist in the determination of current and future NZDF Joint and Single-Service C4I capability requirements for effective coalition interoperability.

THE NEW ZEALAND DEFENCE FORCE OBJECTIVES FOR PARTICIPATION

- Investigate and practice command and control of NZDF force elements within a (simulated) coalition environment.
- Enhance the NZDF profile by demonstrating commitment to coalition interoperability, whilst assisting CWID Allies to achieve their participation objectives.
- Enhance the NZDF C4I knowledge and experience base.
- Identify the utility and applicability to the NZDF of current and emerging C4I systems and applications; and
- Support the Joint Command and Control System (JCCS) acquisition and development process



CWID MANAGEMENT

A CWID Management Team (CMT), co-chaired by the Lead Planner and a representative from the Directorate of Communications and Information Systems Strategy (DCISS), and comprising representatives from HQ NZDF, HQ Joint Forces New Zealand (JFNZ), Joint Information Systems Agency (JISA) and single Services provides planning and management of NZDF CWID activities.

NZDF CWID SPONSOR

Assistant Chief Strategic Commitments and Intelligence (ACSCI) On behalf of the Chief of Defence Force (CDF).

ROYAL NEW ZEALAND AIR FORCE

The RNZAF primary objective for CWID 2007 is to enhance corporate understanding of C4I issues and to identify opportunities that will facilitate more effective RNZAF participation in Joint and Combined operations. In particular, the RNZAF will examine a range of Air C2 tools and enabling technologies to assess their potential for inclusion in the NZDF Joint Command and Control System (JCCS).

RNZAF FOCUS AREAS

- Trials that will enhance Air C4I knowledge and/or contribute to the JCCS
- Trials that support collaborative Air operations planning

RNZAF ACTIVITIES

- Integration of PFPS with ctMPS to facilitate collaborative planning and with C2PC to enhance situational awareness.
- Assessment of Flight Pro by Ocean Software as an enterprise wide Air C2 and squadron management framework.
- Investigation of mobile computing solutions for use aboard non-digital aircraft.

POINTS OF CONTACT

RNZAF PLANNER:
SQNLDR Rob Stockley
PH: +64 4 496 0533
FX: +64 4 496 0538
rob.stockley@nzdf.mil.nz

RNZAF PLANNER AND SITE MANAGER:
SQNLDR Nigel Cooper
PH: + 64 9 417 7000 Ext 7763
FX: + 64 9 417 7738
nigel.cooper@nzdf.mil.nz

RNZAF LEAD ENGINEER:
FGOFF Mike Martin
PH: + 64 9 4177000 Ext 7540
FX: + 64 9 4177808
michael.martin@nzdf.mil.nz

FOCUS FOR THE NEW ZEALAND ARMY, CWID 2007

The NZ Army is establishing a Brigade and deployed Battalion Headquarters at the joint site in Ohakea. The Army's participation is helping to determine the level of digitization required for C2 and situational awareness at the tactical level. The Army will demonstrate network enabling of the new Light Operational Vehicle Command and Control variant, tactical range extension utilizing Satellite Command and Control on the Pause, and EPLRS radios.

NZ ARMY FOCUS AREAS

- Means by which information is communicated collected, stored and displayed.
- Working within a Joint and Coalition environment.
- Structure and procedures required by a networked enabled command post.

NZ ARMY ACTIVITIES

- Integration of technology with the people and procedures required for successful C2.
- Distribution, management, storage and display of information.

POINTS OF CONTACT

ARMY LEAD PLANNER
MAJ Simon O'Neill
PH: +64 21 681 975
FAX: +64 43 87 5561
simon.o'niell@nzdf.mil.nz

SITE MANAGER:
Maj James Dryburgh
PH: +64 4 496-0482
FAX: +64 4 496-0493
james.dryburgh@nzdf.mil.nz

SITE ENGINEERS:
Maj Chris Mortiboy
PH: +64 6 351-9305
christopher.mortiboy@nzdf.mil.nz

WOI Brian Chalmers
PH +64 4 5275-056
brian.chalmers@nzdf.mil.nz

ROYAL NEW ZEALAND NAVY PARTICIPATION IN CWID 2007

The objective for the RNZN will be to investigate technologies with the potential to provide improved collaboration tools for voice and data communication between Force Elements over low bandwidth, high latency, encrypted networks.

POINTS OF CONTACT

RNZN LEAD PLANNER
LTCDR Danny Kaye
Danny.kaye@nzdf.mil.nz

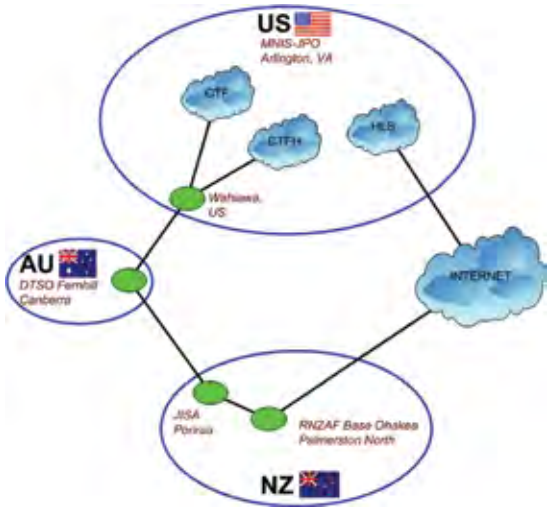
SITE ENGINEER
LT Barry Holmes
Barry.holmes@nzdf.mil.nz

NEW ZEALAND 2007 SITES

The NZDF topology provides sufficient functionality to allow the NZDF to participate within CWID at a national strategic, and deployed tactical Force Element level within real world network constructs and constraints. All CWID 2007 security domains including CTF, CTF High and HS/HD/GOC will be provided in New Zealand with HS/HD/CA being accessed over the Internet via a VPN connection.

■ OHAKEA: RNZAF base Ohakea will host a single site for execution involving Army, Navy and Air elements. Located in the lower North Island the joint site allows each of the three service elements to assess trials that focus on all aspects of the CWID objectives from both a single service and combined operations perspective. The site will be supported by a Network Information Assurance Team providing CND support to the New Zealand segment of the CWID 2007 networks.

■ PORIRUA: The Joint Information Systems Agency (JISA) permanently hosts the Combined Federated Battle Laboratory Network (CFBLNet) Point of Presence (PoP) and manages all linkages from New Zealand to the other participating CWID nations



POINTS OF CONTACT

For more information about NZDFCWID 2007 activities, contact the following:

CWID LEAD PLANNER
LT COL Paul Dragicevich,
RNZSigs, J6
PH: +64 4 529-6600
FX: +64 4 529-6609
paul.dragicevich@nzdf.mil.nz

ENGINEERING LEAD
SQNLDR Stephen Thorpe,
RNZAF
PH: +64 9 417 7000 Ext 7450
FX: +64 9 417 7815
stephen.thorpe@nzdf.mil.nz

ASSESSMENT LEAD
MAJ Simon O'Neill
PH: +64 21 681 975
FX: +64 4 387 5561
simon.o'neill@nzdf.mil.nz

CCEB LEAD
SQNLDR Paul Drysdale, RNZAF
PH: +202 328-4808
FX: +202 265-9238
paul.drysdale@nzdf.mil.nz
nzdscceo@nzdswashington.com

SECURITY LEAD
Ms Katrina Banks
PH: +64 4 496 0165
Katrina.Banks@nzdf.mil.nz

WEB SITES

http://nzdf.mil.nz/cwid (Past, current and future CWID planning information)

http://www.cwid.js.mil

OTHER CWID SITES

The NZDF will deploy Liaison Officers to:

■ CTF (Stuttgart)
■ CFLCC (Dahlgren, VA)
■ CFMCC (San Diego, CA)
■ CFACC (Hanscom AFB MA)
■ UK CWID Site (Portsdown West)

TRIAL PARTICIPATION

TRIAL		DEVELOPER	* TRIAL SECTION PAGE
1.05	Trusted Gateway System (TGS) Guard	US Air Force	3
1.17	Cross Domain Collaborative Information Environment/Collaboration Gateway CDCIE/CG	Trident Systems, Inc., leads more than 12 others	4
1.54	Collaborate-Access-Browse (CAB)	Essex Corporation	5
1.55	Assured File Transfer (AFT)	CTC, Essex Corp., Tresys Technology	6
1.56	Dual Diode (One-Way) Data Transfer System (Dual Diode)	Owl Computing Technologies, Inc.	6
3.09	Global Personnel Recovery System (GPRS)	Innovative Solutions International	12
3.22	Scalable Mesh Networks	OrderOne Networks	13
3.30	Spatio-Temporal Analysis for Rapid Tasking (START)	The MITRE Corporation	14
3.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)	US Air Force, US Navy	16
3.58	US Coast Guard Information Sharing and Communications (USCG IS&C)	US Coast Guard	16
3.70	Coalition open Joint Operations Picture (CoJOP)	Fujitsu Services	17
3.71	MobiKEY Identity Based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	Route1, Inc.	17
3.75	Mobile Tactical Edge Network (MTEN)	Professional Software Engineering, Inc., pTerex LLC	18
3.80	Riverbed Information Optimization System (RIOS)	C2I Solutions, Riverbed	18
5.59	Mission Planning System (MPS)	Collaboration Technologies, Inc.	20
6.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QoS ESI)	DSCI	22
6.15	Geolap	MCE	22
6.74	Security Information Management for Enclave Networks (SIMEN)	The MITRE Corporation	25
6.89	Enhanced Video Text and Audio Processing (eVITAP)	Virage, Inc.	25

*Some technical detail on all trials listed is contained in the back of this Guidebook at the Trials Tab




COMBINED COMMUNICATIONS ELECTRONICS BOARD

Bringing the Network to Life

The United Kingdom's (UK) aim for CWID 2007 is to enhance the interoperability of UK Forces in order to deliver improved military capabilities enabled by networking.

OVERVIEW

This year is the largest CWID so far for the UK with 43 UK trials, seven Coalition trials and seven NATO trials, with over 250 technical and military players operating within the UK alone.

The UK's concept for CWID 07 is to simultaneously demonstrate multiple trials to address Ministry of Defense (MOD) Equipment Programme Capability Gaps, risk reduction activity, industry innovation and coalition interoperability issues. To achieve this, we will link rear based strategic assets direct to tactical platforms, incorporating all strategic, operational and tactical levels of command, as well as connect all domains from above secret to unclassified, all on one network using the current and future Global Communications Network systems. Our main effort is secure interoperability. Our focus being tactical commanders whom require minimum functionality but maximum adaptability.

CWID UK 2007 HEADLINES INCLUDE:

- Resilient Information Infrastructure
- A preview of the Initial State NEC communications infrastructure: integrated end-to-end communications including SKYNET 5, CORMORANT, FALCON, BOWMAN, long-haul HF and TDLs.
- A coherent set of ISTAR trials working throughout the intelligence cycle.
- Risk-reduction activity in support of a variety of funded programmes including: aircraft mission planning systems such as the Joint Combat Aircraft; the Joint Effects Tactical Targeting System; BOWMAN CIP 6; and the future LCC C2 system for the ARRC.
- A variety of demonstrations addressing-current capability gaps, including in the areas of airborne Tactical Data Links; Service Oriented Architecture; Information Management; Joint Operational Picture; coalition interoperability.

Within the UK the demonstration will be conducted on a secure, web based, open Service Orientated Architecture using IP as standard using real data, passing over real bearers (including satellite and long range HF) employing real MOD security for military role players to use and assess. This network will mirror not only the current deployment but also the future vision of the UK's Global Information Infrastructure. All trials will undergo user, technical and capability assessment led by CWID staff.

UK NATIONAL LEAD

Wg Cdr Stephen Borthwick RAF
SO1 NEC / CWID
DEC CCII
Ministry of Defence
+44 207 807 8526
stephen.borthwick538@mod.uk

UK NATIONAL COORDINATOR & SCENARIO LEAD

Maj Gavin Saunders PWRR
SO2 CWID
DEC CCII
Ministry of Defence
+44 2392 217657
gavin.saunders217@mod.uk

UK TRIALS COORDINATOR

WO1 Carl Allison RA
SO3 CWID
DEC CCII
Ministry of Defence
+44 2392 217715

TECHNICAL LEAD

Viv Danks
Team Leader
Deployed Network Solutions QinetiQ
+44 1684 896891
vgdanks@qinetiq.com

SECURITY LEAD

Peter Smulovic
CWID Project Manager
DSTL
+44 2392 217458
psmulovic@dstl.gov.uk

ASSESSMENT LEAD

Louise Orpin
Land Systems Assessment
DSTL
+44 2392 912274
ljorpin@dstl.gov.uk

FACILITY MANAGER

Nicola Grimes
Mercury Building Manager
DSTL
+44 2392 917506
njgrimes@dstl.gov.uk

TRIAL INTEROPERABILITY

The UK is committed to meaningful participation in CWID as part of our programme to improve interoperability in a coalition context: a very high priority task. Our trials rely on data derived from the coalition Wide Area Network (WAN). In addition, the UK is an active participant in both US and NATO CWID either by providing trials/demonstrations in the US or at Lillehammer, or by contributing to data on the coalition WAN. Each trial will exchange live data at either the national or coalition level through the period of the demonstration. It is important for the UK that the network used is fully security accreditable, as it carries real data.

LOCATION

The principal UK CWID site is located at Portsdown West, the Defence Science and Technology Laboratory's site near Portsmouth in the South of England.

OWNERSHIP

UK involvement in CWID is sponsored by the 2-star Capability Manager (Information Superiority), Air Vice-Marshal Stuart Butler,

and responsibility for delivering the programme lies with the 1-star Director Equipment Capability (Command Control and Information Infrastructure), Brigadier Simon Shadbolt.

BENEFITS

CWID benefits industry, the MOD and wider Government. Direct benefits are potential solutions for capability gaps, risk reduction activity supporting currently funded projects, or the support to innovation and experimentation. Indirect benefits for both UK MOD and industry are: technical and financial leverage; user opportunities such as training and policy assessment; as well partnership development and project exposure.

As we continue to develop the crucial Network Enabled Capability (NEC) required by our armed forces in the years ahead, CWID has the potential to assume ever greater importance, not only in resolving interoperability issues but also in reducing the degree of risk inherent in all such programmes.

RELATED WEBSITES

The UK CWID website at **www.cwid.org.uk** contains further information about UK CWID 2007, including descriptions of trials.

VISITORS

Visitors' Week for CWID in the UK will take place at Portsdown West over the period 15-22 June 2007. Anyone wishing to visit should apply via the UK CWID website.

INDUSTRY PARTNERS

The UK acknowledges the active participation of a large number of MOD and industrial partners, many of whom have trials at US, UK and/or NATO CWID sites.

The Defence Science and Technology Laboratory, Dstl, is contracted to host the UK CWID site and provide facilities, security and assessment of UK and Coalition trials. QinetiQ is contracted to provide the UK CWID network and manage its connections to the coalition network. In addition, UK CWID receives valuable contributions from industry partners, who, whilst not exhibiting trials in the US, provide a significant input to the US planning conferences, helping to ensure the success of CWID.

QinetiQ has been instrumental since 2000 in designing and delivering the UK Secure

QinetiQ WADI helping to enable NEC

DEFENCE SCIENCE AND TECHNOLOGY LABORATORY [Dstl] is a UK Ministry of Defence (MOD) facility. Apart from the site and infrastructure, Dstl also provides: links to CFBL Net; associated cryptographic devices; equipment; and personnel to support the QinetiQ CWID technical team. Dstl also provides the assessment, administration, catering and security to support both CWID and the associated visitors' programme. Contact Details: psmulovic@dstl.gov.uk

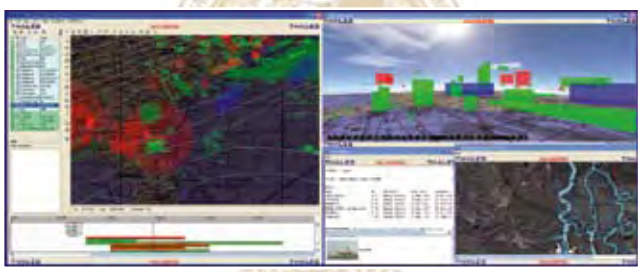
Network for JWID/CWID. This has been delivered using the Wide Area Distributed Infrastructure (WADI) Solution.

Thales Air Operations celebrates its sixth year of participation in the JWID/CWID programme. In addition, the company has supported the UK CWID team throughout all UK and US planning conferences since 2002, contributing to scenario and Air Tasking Order/ Airspace Control Order (ATO/ ACO) production.

BAE Systems INSYTE will perform the role of System Integration for the ISTAR trials and demonstrations for CWID 2007 in the UK. The demonstration shows the interoperation of D3 products in separate security domains.

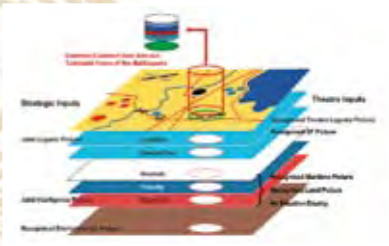
Fujitsu is participating in US CWID with its Coalition Open JOP (CoJOP) that is also registered in the NATO CWID.

These trials, which have UK national equivalents, interface with coalition partners and are information providers to the UK openJOP, providing shared situational awareness.



Thales Air Operations

BAE Systems



Fujitsu

United Kingdom Trials Matrix

TRIAL ID	TITLE	COMPANY/ ORGANISATION	POINT OF CONTACT	POINT OF CONTACT E-MAIL ADDRESS
UKIT01	Provision of the real-time link 16 air picture into UK CWID	Aerosystems International	Phil Short	Phil.Short@aeroint.com
UKIT02	Air SA Gateway Link – C2IEDM	Aerosystems International	Phil Short	Phil.Short@aeroint.com
UKIT03	Rotary MPS & Airborne CP	Augusta Westland	Brian Armstrong	brian.armstrong@augustawestland.com
UKIT04	ISTAR Afloat – Enabling Maritime Intelligence	BAE Systems INSYTE	John Loader	John.loader@baesystems.com
UKIT06	FALCON – Enabling Battlespace Intelligence	BAE Systems INSYTE	John Loader	John.loader@baesystems.com
UKIT10	ISTAR Deployed – Providing Battlespace Intelligence	BAE Systems Insyte	John Loader	John.loader@baesystems.com
UKIT17	Security Labelling From Text Labels to x.841 labels	Clearswift	Jim Craigie	Jim.craigie@clearswift.com
UKIT20	MANPADS Threat Assessment Tool (SAMPRAS)	Cunning Running Software Ltd	Chris Barrington Brown	b_b@cunningrunning.co.uk
UKIT26	Agile JOP	EDS Defence Ltd	Steve Fearnley	steve.fearnley@eds.com
UKIT30	Enhanced ASH EOD and NBC BISA Interoperability for Operational Users	EDS Defence Ltd	Nick Hill	nick.hill@eds.com
UKIT31	Prototype ISTAR Toolkit Intelligence collection and requirements management	EDS Defence Ltd	Alan King	alan.king@eds.com
UKIT37	Semantic open JOP	Fujitsu Services	Kevin Parry	kevin.parry@uk.fujitsu.com
UKIT38	Joint Task Management Tool	Fujitsu Services	Kevin Parry	kevin.parry@uk.fujitsu.com
UKIT39	Air Component ToolSet	Fujitsu Services	Kevin Parry	kevin.parry@uk.fujitsu.com
UKIT41	BCIP 5 Land Environment Interoperability	General Dynamics	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
UKIT42	BowmanCIP 6 Risk Reduction	General Dynamics	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
UKIT43	Airborne NEC TADIL integration with GII	General Dynamics	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
UKIT44	MEC Exploitation System of Systems	General Dynamics	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
UKIT45	Future Information Capability	General Dynamics	Jeremy Creasey	Jeremy.creasey@generaldynamics.uk.com
UKIT46	Delivering a core service capability for agile command and control for NEC	IBM	David Farquharson	David.farquharson@uk.ibm.com
UKIT47	MoD Geoint Provision	Intelligence Collection Group	Maj Fennell	icg-randdso2@icg.mod.uk
UKIT48	JCA Off board Mission Support Interoperability with UK infrastructure and UK mission planning systems	JCA, IPT, DPA	Sqn Ldr Bob Arber	bob@bjarber.plus.com
UKIT51	Secure & Assured Core Defence Network – Protecting The Information Chain	Juniper	Tim Hearn	thearn@juniper.net

TRIAL ID	TITLE	COMPANY/ ORGANISATION	POINT OF CONTACT	POINT OF CONTACT E-MAIL ADDRESS
UKIT53	Deployable IM/IX	Lockheed Martin	Stephen Hastings	stephen.j.hastings@lmco.com
UKIT55	Deployed tactical video surveillance management and assessment system	Lockheed Martin	Stephen Hastings	stephen.j.hastings@lmco.com
UKIT62	Secure Guarding of Interconnected Domains	Nexor	Steve Penny	steve.penny@nexor.com
UKIT66	Satellite Information Dissemination Service using Skynet 5	Paradigm	Ken Hadfield	ken.hadfield@paradigmservices.com
UKIT68	Defence Core Information Management Capability	QinetiQ	Mike Farrington	mfarrington@qinetiq.com
UKIT69	IP optimised maritime HF communications	QinetiQ	John Spencer	JASPENCER1@qinetiq.com
UKIT70	Joint Effects Tactical Targeting System (JETTS)	Raytheon Systems Ltd	George McFarlane	george.mcfarlane@raytheon.co.uk
UKIT73	Air-Land Situational Awareness over long range wireless LAN	Rockwell Collins UK Ltd	Bill Mackenzie	wdmacken@rockwellcollins.com
UKIT76	Information dissemination over multiple bearers including HF	Selex Communications	Tim Merriman	tim.merriman@selex-comm.com
UKIT79	Intelligence-guidance Computer Network Defence	Symantec UK Ltd	John Ellis	john_ellis@symantec.com
UKIT80	COSMOS multi-national data repository and gateway	Systematic Software Engineering Ltd	Ian Smart	ian.smart@systematic.co.uk
UKIT81	Combined C2 Information Web Service	Systematic Software Engineering Ltd	Paula Miller	paula.miller@systematic.co.uk
UKIT82	Coalition Infrared Data Processing	USAF S&MC	Maj Marcus Chaney	mark.chaney@buckley.af.mil
UKIT84	Web Service Delivery of Tactical Decision Aids (Maritime)	TENET Defence Ltd	John Tate	john.tate@tenettechnology.com
UKIT85	Provision of Dynamic Environmental Information via JEDDS	The Met Office	Jeff Osbourne	jeff.osbourne@metoffice.gov.uk
UKIT86	FIMMA Integrated multi-platform / role mission management system	Thales Air Operation	Martin Boughen	martin.boughen@uk.thalesgroup.com
UKIT87	JEDDI Middleware	Thales Air Operation	Martin Boughen	martin.boughen@uk.thalesgroup.com
UKIT89	Dissemination and collection of Tactical ISTAR Imagery to and from a deployed AFV	Thales	Ian James	Ian.james@uk.thalesgroup.com
UKIT90	Joint Reconnaissance Pod Ground Station Connectivity	Thales	Paul Varney	paul.varney@uk.thalesgroup.com
UKIT93	Migration of ARRC C2IS to UK LC2IS	Thales Joint Systems	Paul Baller	Paul.baller@uk.thalesgroup.com

US INTEROPERABILITY TRIALS			*PAGE
IT5.08	Joint Strike Fighter Offboard Mission Support Environment (JSF OMSE)	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	19
IT3.14	Coalition Secure Management and Operations System (COSMOS)	Booz Allen Hamilton	12
IT6.15	Geolap	MCE	22
IT2.21	Commercial Joint Mapping Tool Kit (CJMTK)	Northrop Grumman Corp.	10
IT3.31	Coalition Infrared Data Processing (CIDP)	The Aerospace Company	14
IT3.70	Coalition open Joint Operations Picture (Co-JOP)	Fujitsu Services	17
IT2.88	Adlib	EchoStorm, Inc.	11

NATO TRIALS		
NUK 8	Deep Secure	Clearswift
NUK 9	Directory Bastion	Clearswift
NUK 10	SNMP Bastion	Clearswift
NUK 95	Corporate Intelligence Led CND	Symantec
NUK 97	Coalition C2 Info Webshare	Systematic Software Engineering
NUK 99	Coalition Open Joint Operational Picture	Fujitsu Services
NUK100	Air Component Tool Set	Fujitsu Services

*Some technical detail on US trials listed is contained in the back of this Guidebook at the Trials Tab

NORTH ATLANTIC TREATY ORGANISATION

Toward Decision Superiority

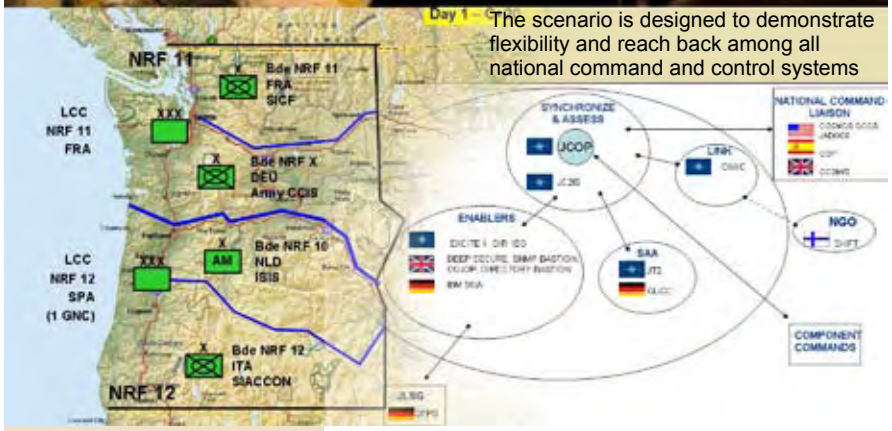
The NATO Coalition Warrior Interoperability Demonstration (CWID) is an annual NATO Military Committee approved event designed to bring about continuous improvement in interoperability for the Alliance. Allied Command Transformation (ACT) provides direction and management to the programme, while NATO and Partner nations sponsor interoperability trials with specific objectives defined by ACT and National Leads.

The shared vision of the two Strategic Commands (Allied Command Operations and Allied Command Transformation) is that NATO forces, including the NRF, achieve a state of Decision Superiority that in turn is enabled by achieving Information Superiority through networked forces. Allied Command Transformation (ACT) is therefore engaged in efforts to create forces that are capable of achieving this type of Decision Superiority. ACT is driving the development of concepts and systems that can achieve Information Superiority, and are tested and validated using the full spectrum of available exercises, trials, and experiments – such as CWID.

NATO CWID 2007

The NATO CWID programme focuses primarily on testing and improving the interoperability of NATO and national C4I systems, with particular emphasis on those that would be deployed within a NATO Response Force or Combined Joint Task Force. In addition to bilateral technical testing, NATO CWID provides a venue to conduct technical testing of fielded, developmental and experimental systems in the context of a coalition scenario. The event runs concurrent and shares elements of a common scenario with the Chairman of the U.S. Joint Chiefs of Staff CWID annual event.

The operational commitments for these NRFs commence in July 2008 and as such, any interoperability issues that are identified as a result of trials conducted in CWID can be addressed and resolved prior to that time.



The scenario is designed to demonstrate flexibility and reach back among all national command and control systems

POINTS OF CONTACT ACT/C4I

Cmdr. Clark Price
NATO CWID Director
cprice@act.nato.int
+1 757 445 3556

Mr. D.C. Taylor
NATO CWID Deputy Director
dtaylor@act.nato.int
+1 757 445 3556

NATO CWID EXECUTION SITE

The primary NATO CWID 2007 execution site is at the Norwegian CIS Center of Excellence near Lillehammer, Norway. The Camp has a military history dating back to 1750 and has been in use by the Norwegian Army Signal Corps since 1945. The Camp was selected by the Norwegian parliament

to be the site of the Joint CIS Training Centre within Norway. The Camp has taken on this new role, which compliments the Joint and Coalition nature of the testing that will be conducted in CWID 2007.

NETWORK TOPOLOGY, NATO DOMAIN, LILLEHAMMER

The NATO CWID 2007 network at Camp Jorstadmoen is built around a common domain referred to as the Coalition Task Force (CTF) / NATO Response Force (NRF) domain. NATO CWID network architecture has its primary site at Camp Jorstadmoen. The diagram on the right depicts additional national sites used in conjunction with NATO CWID tests which are conducted remotely.

Several nations use Information Exchange Gateways (IEGs) to separate their national LANs from the common domain, thereby analyzing the interoperability over their cross-domain solutions. Below is a logical overview of the network in Lillehammer.

PARTICIPATING NATIONS AND AGENCIES

There will be 17 nations and agencies actively participating from the NATO execution site in Lillehammer and an additional 3 nations who will attend as observers. NATO will participate with C2 systems from each of the operational environments: the Maritime MCCIS, Air ICC and Land LCCIS.

THE NATO SCENARIO AND NRF STRUCTURE

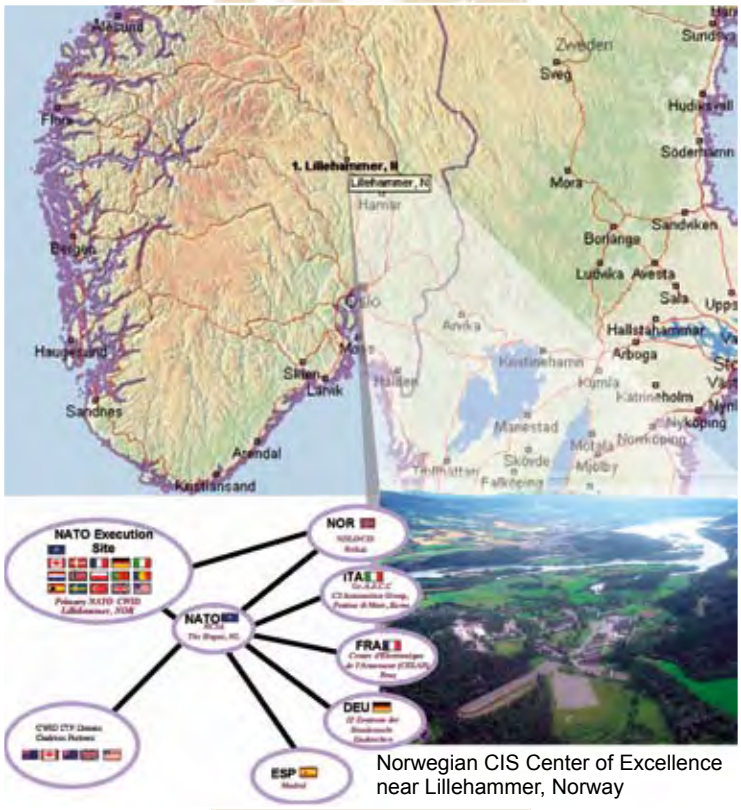
The NATO Scenario was designed for the NATO Response Force, which is driven by the underlying principles: "first force in, first force out" and tailored for specific missions. The NRF is capable of performing certain missions on its own, as well as participating with the US CTF. Deployed as a standalone force for Crisis Response, the NRF is expected to be able to respond to the following events:

- Evacuate non combatants from crisis area
- Support consequence management (including chemical, biological, radiological and nuclear incidents)
- Support in a humanitarian crisis situation
- Manage crisis response operations, including peacekeeping
- Counter terrorism operations
- Embargo operations

NATO Response Force (NRF) is driven by underlying principles: "first force in, first force out" and tailored for specific missions.

The NATO Scenario's flexibility provides the ability to be tailored to test the interoperability of the various national Command and Control systems as well as individual C4ISR trials. For 2007, Joint Command Lisbon is spearheading NRF rotations 11 and 12 efforts. In response to the changing needs of the NRF, the headquarters structure is loosely based on an Effects Based Approach to Operations (EBAO).

This structure reflects the requirement to deploy a forward command element with the capability to reach back to the larger headquarters' staff. The diagram on page 13 showcases the forward command element with the capability to reach back to the headquarters element along with other outside elements.



Norwegian CIS Center of Excellence near Lillehammer, Norway

2007 NATO OBJECTIVES

IThree objectives have been identified as major priorities for NATO CWID 2007:

OBJECTIVE 1: Conduct testing, in support of certification, to assess the interoperability between CIS Systems required in NRFs 11 and 12 based on information exchange requirements and interoperability test requirements.

OBJECTIVE 2: Conduct testing in support of NNEC by providing tools to facilitate the management of information, enabling automatic discovery and integration technologies which promote loose coupling between systems and components, and test and explore web-based Service Oriented Architecure (SOA).

OBJECTIVE 3: Test and assess the interoperablity of systems supporting current NATO operations.

The NRF **AIR COMPONENT** structure allows for the interoperability testing of a deployed Combined Air Operations Center (CAOC) and associated control cells.

The **LAND COMPONENT** for the NRF contains a structure sufficient to allow deployment of a tailored brigade size formation composed of manoeuvre elements and the requisite assets to allow it to conduct a wide range of land tasks. In CWID, the land component structure allows for interoperability testing between command and control systems that use both Multilateral Interoperability Program (MIP) and ADatP-3 formats.

The NRF **MARITIME COMPONENT** will comprise a force of multiple NATO task forces including a carrier battle group with associated surface and subsurface combat units, amphibious forces, naval MCM units and auxiliary support vessels. Although, a force this large would not normally deploy as an NRF it allows for interoperability testing between various maritime command and control systems.

NATO Interoperability Trials and Demonstrations

CANADA	
TBMCS/ACCS	IT and ID which tests and evaluates exchange of information such as ATO, ACO, Tracks data, RAP and other information available on the web servcices.
DENMARK	
DNK C4I C-Flex	Experimental test of strategic & tactical interoperability of C-Flex (new Royal Danish Navy C4I system) and experimental testing of the emerging NATO Blue Force Tracking capability (NATO BFTSA II) with army units.
DNK – DACCIS	DACCIS multi-level army C2 System designed to assist planning, execution, information gathering and decision-making processes within division, brigade and battalion HQ during army operations
DNK-NMS	NMS system for planning, executing and monitoring mobile networks and includes C2, own and enemy situation picture.
FINLAND	
FIN-AHJO	AHJO is Fire Control and Information System for Finnish Army. IAHJO maintains and exchanges Army COP for artillery and mortar units.
FIN-STROP	STROP is a Joint COP (Army, Navy, Air Force) experiment.
FIN-SHIFT	SHIFT provides for information interoperability (currently MIP block2 and XML in SOA/ESB bus), situational awareness (currently COP and CIMIC information) and tools for collaboration for creating and exchanging both COP and CIMIC information.
FRANCE	
FRA-SCCOA	ITest Exchanges supporting Planning, Tasking and Current operations management of missions at JFAC/HQ and CAOC levels.
FRA-BFT	ID of EADS Imp@act Blue Force Tracking System. Tracks are exchanged and displayed between BFT systems from different nations, through a specific tracks exchange interface (NFFI)
FRA-SAIS	ID of technical services through a Littoral Warfare scenario. Supports an international Services Oriented Architecture (SOA), which provides Network-Centric Capabilities.
FRA-SIC21	IT of the French Maritime C2I system within the NATO scenario.
FRA- T-BMS	NFFI Exchange and Messages Exchanges, Graphical situation follow-up on digitized maps, testing the implementation of NFFI 1.3 protocol
FRA-SICF T-BMS	SICF exchanges messages with the MCC, the ACC and the SOCC using appropriate ADatP-3 messages that are automatically synthetized and analyzed by the system. SICF receives and displays NFFI tracks.
FRA-MAESTRO	Maestro is the fielded C2 system of the French special Forces and French Battalions of the French/German Brigade
FRA-SIR	Coalition blue force tracking capacity included in the FR battalion C2 system. SIR will include a coalition blue force tracking capacity where tracks are exchanged between the SIR and other coalition units, based on the NFFI V1.3.1 standard.
GERMANY	
GER-ADLER II	Prove capability to conduct target acquisition and fire support via IP Networks applying the ASCA Interface. Transmit supporting visual information (video and images).
GER-Army CCIS	German Brigade HQ / LCC within NRF: Distribution of situational data for creation of dynamic CROP (sceanrio play) and transmission of simulated BFTS-Data for Force-Tracking-Experiments via NFFI-Gateway.
GER-IBM SOA	Secure exchange of MIP, ADatP-3, TDL messages between different C2IS systems and security domains.
GER-CLiCC	Test collaborative work of intelligence centers to enhance Situational Awareness by means of real-time CROP. Test formatted and unformatted documents from various sources. Provide Integrated Services for Data Fusion, Situation Assessment and ISR Dissemination.
GER-DIG	Domain Specific Information Generator (DIG, product name SIENA) which composes and executes real-time crisis scenarios thus providing real-time and realistic ADatP-3 formatted Situation Report messages (OWNSITREP, ENSITREP) and Intelligence messages (INTREP).
GER-Geoinformation Services	Bundeswehr Geoinformation Office provides geospatial and METOC data into a classified network. After data collection and evaluation a Recognised Environmental Picture (REP) is generated and provided as Web-Services.
GER-HEROS	ADatP-3 (BL 12.2) based Information exchange between the GE C3I system HEROS and other MIP conform C2IS. The Information exchange between HEROS and other MIP C2IS using standard protocol TCP/IP; MIP Data Exchange Mechanism (DEM) and C2 Information Exchange Data Model, C2IEDM
GER-ICARUS	Test information exchange with land units via message exchange (ADatp-3, OTH-Gold) and/or MIP DEM
GER-IEG GAFCCIS	Test functionality of selected software, hardware and concept for the GAFCCIS IEG to exchange military information with NATO & NATO nations as i.e. ADatP-3/XML-MTF formatted messages or directory information.
GER-Link 16	Demonstrate ability to communicate with ACC LOC 1 and Mobile SAMOC to exchange RAP-Data using Link-16. Evaluate the ability to exchange data in ADatP-3 Format
GER-SAMOS	EADS-Germany will connect to the L 16 SIMPLE-network, allowing full situational awareness with ACCS Log1, MEADS, ICC; F124 etc. SAMOC is the coordination of subordinate weapon systems. Additionally SAMOC provides ADatP-3 for non-real-time data exchange.
GER-MOFS-SNR	Mobile Forces Solution - Secure broadband satellite communication to ship and secure SubNet Relay via HF/UHF and DVB-T.

GER-SAP-DFPS ERP-C2IS	IData transfer from ERP-System to CCIS andupdate of CCIS with real time logistics information. Test and demonstrate ADatP-3, MIP and WebServices interfaces. Test and demonstrate interfaces to LogFAS (LOGREP/ADAMS).
GER-MiLiPos	Interoperability Demonstration a generic approach to process Link Data on the way to development of a Common Message Standard (CMS). MiLiPos provides an interconnection between Link 16, Link 22 and LLAPI (RAP, RGP) and C2-InfoSystems.
ITALY	
ITA-BFT	Blue Force Tracking Tool used at tactical level to provide situational awareness of Land/Joint Units and Intelligence units. Provides basic geographic information and helpful tools to export positional data to C2 Systems
ITA-C4I Defense	C4I Defense, Italy Joint System, provides top-level strategic capabilities, laying above the tactical functionalities offered by the CC systems of each Armed Force. It supports the Operational Commander in Operations Planning and Tasking (Orders Generation) and in Tactical Situation Analysis and Monitoring.
ITA-ICISRC	IT_JOISRC provides pre-exploited GMTI (Ground Moving Target Indicator) and ESM (Electronic Support Measures) data to ISR (Intelligence, Surveillance and Reconnaissance)network and exploited ISR information to both ISR network and C2 systems in order to increase situational awareness and to assist Strategic, Operational and Tactical Commanders (and their Staffs) in decision making processes.
ITA – Link 16	The aim of trial is to TX and RX the tactical picture of Link 16 (and other TDL) through satellite or land IP network by connecting one Workstation at NATO Test site and to a US Coalition workstation able to exchange JREAP-C traffic.
ITA– IEG B	ITest of the Italian IEG case B first prototype. The architecture and principles are derived from NATO NC3A directives.
ITA – BFSA	Italy Blue Force Situation Awareness is a tactical level system to provide Situational Awareness of Land Units through automatic dissemination of information using different types of communication media. It provides functionalities to exchange messages and alarms among Units and manage geographic informating using a Geographic Information System. Aim is to test the new interoperability features of the system based on NFFI specification Version 1.3../ Draft STANAG 5527
ITA – IPv6 Architecture	Demonstrate feasibility of operating national C2 systems over (or through) an IPv6 based network.
ITA – SIACCON 1AW + PSOT	Army C2 system to support Commander's Analysis of Tactical Situation, Mission Planning, Orders and Directives Handling and operation monitoring. SIACCON allows information exchange and RGP Sharing with NATO/PfP Joint & Single service C2 System. PSO Tools (Peace Support Operations)support CIMIC and Peace Support activities providing a number of functionalities to Italian Army C2 System SIACCON , to increase the automatization, reliability and effectiveness of operations.
ITA– SiCCAM	Italian Air Force C2 System provides capability of air operation planning and tasking, RASP reception and forwarding, military message handling and air bases management. It also can do resource management and Current Operations management.
NATO	
NATO-ACCS LOC 1	ACCS ID is designed and developed to support the planning, tasking, execution and reporting of combined joint air operations.
NATO – SAIA	Improve the Information Assurance Situational Picture by collecting sensor information and translating the data into a standard specification which can be fed into a central management system.
NATO – JC2IS	NATO JC2IS provide Joint C2 Services for the NATO levels of command in multi-national coalition based operations and is closely related to the NATO JCOP. NATO JC2IS supports Joint Functions (e.g. Targeting, CIMIC, Engineers, Event Logging) and has the capability to exchange the relevant information products with the NATO JCOP service
NATO – EXCITE II	EXCITE II (Extensible XML-based C2 Collaboration and Coordination Information Exchange Tools Environment) uses C2 coordination tools to pass information, coordinate operations and support collaborative decision-making in real-time.
NATO – CDWS	Web Services (WS) used to implement a Service Oriented Architecture (SOA). SOA are of particular interest with respect to the achieve the envisaged Network Enabled Capabilities (NNEC) in future. The trial will use the XML security labels as specified by NC3A and previously tested in CWID in combination with a XML security labelling guard prototype to facilitate cross-domain exchange of SOAP messages through the guard.
NATO – IEG	NATO IEG will provide IEG scenarios B/C/D. For B/C the main focus will be demonstrating interoperabilty of the collective services. For scenario D the main focus will be to develop the technology for enhanced CIMIC.
NATO– IEG FS	Assess cross-domain interoperability with C2 systems supporting (T)DL standards; assess cross-domain interoperability with XMPP tools, both server-to-server and client-to-server; test functionality of labelling mechanism, sanitization mechanism, signing mechanism, guarding and data integrity and test the delay introduced by the different implementations of the IEG-FS for the different scenario, measuring throughput.
NATO – BFSA III	This trial will build on NBFSA-II achievements and address additional interoperability issues that need further experimentation.
NATO – CIMIC	Demonstrate data communications between military and civil users, using NATO provided network and existing civil and military terminals; develop and exploit a proof of concept Information Exchange Gateway (IEG) for CIMIC applications for a Civil entity willing to use NATO provided systems e.g. national government, UN as well as a Civil entity unwilling to use NATO provided services e.g. NGOs, ICRC
NATO – JTS	JTS is the main information provider in the NATO targeting domain. JTS supports the full targeting cyle including joint target list (JTL), prioritised target List (PTL), prohibited target list (PrTL), etc. To enhance the data descriptive enough to practise targeting, JTS tools can be used to fill out target data, identify DMPIs, find appropriate weaponeering solutions and add imagery for some targets.
NATO – ICC281	ICC (NATO-wide Integrated Command and Control Software for Air Operations) provides powerful tools for planning, tasking, reporting and situational awareness.
NATO - NEC CCIS	NEC CCIS is a NATO non-real time Command and Control system, mainly used for air operations in Denmark and Norway, including CAOC1 and CAOC3. Using a standard three-tier architecture, the NEC CCIS users work with a distributed database through a client application running on their Windows workstations. Using NEC CCIS, the operational users get access to operational services such as Air space management, Air planning, Air current operations, Targeting, Squadron operations (fighter, helicopter, GBAD), Rules of Engagement/NATO Crisis Response System/Alert management, Logistics, Intel, system administration, security administration.

NATO – ACCS-LSID TMD	ACCS-LSID TMD capability with national TMD weapon, sensor, and BMC3I systems. The activity will focus on the exchange of TMD situational awareness (SA) data between the ACCS Reduced Version HW/SW suite (with LSID) and national system(s) capable of providing TMD associated SA data (e.g., tracks, weapon system status, engagement status, etc.) The objective is to demonstrate an interim NATO capability to display TMD SA data provided by national systems, as well as to provide risk mitigation for the development of ACCS related TMD interoperability requirements being generated by the ALTBMD PO.
NATO –NMS Evolution	Test of PKI, directory service and messaging interoperability including, desktop-to-gateway, gateway-to-gateway in accordance with the ACP145 NATO Supplement under development, and desktop-to-desktop.
NATO – NMS Interoperability	Test of NMS components within a NATO organizational structure, engineered with Phase 2 enhancements. NMS components will also be installed in the NATO-led CJTF and configured with the mission security policy. An IEG will be used to control the exchange of message and directory information between the two security domains.
NATO – SBC	Server Based Computing Element will implement thin-client technologies and focus on rendering typical NRF core and functional services using SBC and assessing performance over SatCom links from an operational perspective.
NATO – ICC	ICC (NATO-wide Integrated Command and Control Software for Air Operations) provides powerful tools for planning, tasking, reporting and situational awareness
NETHERLANDS	
NLD-ISIS	C2 system for headquarters and other semi-static Command elements for landbased operations of the Netherlands MOD. Povides a Common Operational Picture (COP) to create shared awareness in operations
NORWAY	
NOR-NORCCIS	ICHOD Norway's primary Command and Control system for support of Joint operational and tactical levels of operations.
NOR-NORTaC C2IS	Norway's primary Command and Control system for tactical land operations from Div to Bn level using MIP DEM block 2.
NOR-SecSOA	The trial will focus on security labelling and filtering of Web Services traffic using an XML Guard
NOR-BFSA NFFI	This trial will build on blue force situational awareness work from CWID 06 based on NATO's NFFI specifications.
NOR- CIAT	NODSA will perform as Coalition Information Assurance Team lead at Base Jorstadmoen by deploying network intrusion detection systems at the core-network, monitor for intrusions, malware and other misuses/policy violations.
NOR-NEC CCIS	NEC CCIS is a NATO non-real time Command and Control system, mainly used for air operations in Denmark and Norway, including CAOC1 and CAOC3. Using a standard three-tier architecture, the NEC CCIS users work with a distributed database through a client application running on their Windows workstations.
POLAND	
POL-SAMOC	Demonstrate the ability of cooperation between Polish SAM OC and ICC and ACCS during air defence cluster planning (MEZ) and during defence of MEZ zone.
POL-SZAFRAN	Tactical Command and Control Information System SZAFRAN supports the planning and control of Army operations on corps, division, brigade and battalion level, and the exchange of information among national and allied command posts.
POL-AOCC	Verify exchange of ACo,ATO, OWNSITREP, ENSITREP, AIRREQ, ACMREQ. Polish AOCC (PODBIAL) is dedicated to support joint operation between land and air forces and between maritime and air forces.
PORTUGAL	
PRT-SICCE	Battalion and above level system designed to interoperate with other C2 systems using MIP specifications. SICCE can exchange tactical information between national and coalition partners according to MIP baseline 2 specifications.
PRT-RMPoHF	Present and test the architecture adopted by PRT Navy to manage and broadcast the RMP using HF Band.
ROMANIA	
ROU-SIAAB	Battle C2 system designed for command posts and units operating at the tactical level (Brigade and Battalion). The system has 4 main categories of services: MIP, MMHS, Security (PKI, Directory, OCSP and Single Sign One), and GIS.
ROU- SICIB	SICIB provides interoperability with the coalition's C2 information systems using: MIP MEM, NFFI mechanisms for the Battalion and lower levels; and MIP MEM, MIP DEM, NFFI for the Battalion and higher levels.
SPAIN	
ESP-AT12	ID of an Advanced Trusted Information Interoperability demonstrator that enables secure the data exchange between Nations using the new Web Services technology in a trust common environment.
ESP _SIMACOP	Test the interoperability of the C4ISR SIMACOP © with other relevant C2IS or blue force tracking systems.
ESP-AMERHIS	Demonstration of the advantages of using Regenerative Satellite Communication links with On-board processing for military communication applications.
ESP-COP	Show a Common Operational Picture created with information coming from national sources through a web browser. To provide web services to other C2 IS that could require information. To use any web services provided by other C2 IS.
ESP- SIEMENFAS	Exchange messages with partners using different MMHS (Military Message Handling System) based on STANAG 4406. The purpose is to have a MTA (Message Transfer Agent ie. a message server) and several UA's (User agents ie message clients) to test exchanging of military messages (P772 format, defined in the ST 4406) with other national implementations (or pilots) of ST 4406 systems.
SWEDEN	
SWE-IS SWERAP NBG	IS SWERAP NBG will be the C2-system fielded in the EU Nordic Battle Group 2008. Capabilities include MIP Block 2 and ADatP-3 situational awareness. IT and ID of a developmental system for the EU Nordic BG HQ in 2008.
SWE-IS SWERAP CWID 07	IS SWERAP CWID 07 will be used exclusively for Interoperability Experimentation. The basic configuration is according to IS SWERAP NBG, but additional capabilities in different service areas will be added.

SWE- IS SWERAP FAS CBRN NBG	NBC related information exchange in a coalition framework. Capabilities include Functional Area Support and ADatP-3 message exchange.
SWE-A3A	ADatP-3 message handling capability for the Swedish Air Force. A3A uses dynamic message forms and powerful GIS tools to present ADatP-3 message information allowing the user to interact with ADatP-3 message information.
TURKEY	
TUR-IEG	IEG used for information sharing implementations among different security domains. Different technical implementations and use of commercial products are applicable. Design alternatives will be tested before deployment.
TUR-Navy IP over HF	Turkish Naval Forces and a national institute (TUBITAK) developed a national STANAG 5066-compliant IP over HF system named FORESC. In CWID 2006, tests were conducted among Turkey, Spain and Norway. Limited success was the result of the tests. As for the lessons learned at CWID 2006, Turkish Naval Forces has made some modifications in FORESC. Turkish Naval Forces wants to conduct tests with other nations' IP over HF systems both in uncrypted and crypted modes to check the results of the modifications that have been made to FORESC.
TUR-OMEGA	Turkish Naval Forces strategic CCIS system OMEGA has the capability of processing ADatP-3 B.11 and B 12.2 NAVSITREP and NAVSITSUM messages and OTH-T GOLD CTC messages.
TUR-TAF CCIS	TAF-CCIS is the Turkish Armed Forces (TAF) joint C2 system which constitutes an integrated representation of information along with the allied, neutral, and enemy units of the army, navy, and air force.
TUR-TICCS	TICCS is Integrated Command and Control System of Turkish Air Force. It includes Battle Mgmt, Resource Mgmt, and Documentation Mgmt Subsystems. ID of TICCS: Integrated Command and Control System of Turkish Air Force that includes Battle Mgmt, Resource Mgmt, and Documentation Mgmt Subsystems.
TUR-TACCIS	TACCIS (Tactical Area Command and Control Information System) is a situational awareness and decision making tool within NRDC-T and its subordinates. The primary use of TACCIS is to develop, view and analyse Order Of Battle (ORBAT) information using a Geographic Information System (GIS) as the background to form the Common Operational Picture (COP). Basic system components of TACCIS are; operational database, Geographic Information System (GIS) database, Database Replication Mechanism, Message and Crises Management system and an application software. It is a fully MIP compliant and certified CCIS
UNITED KINGDOM	
GBR – BCIP6	Tactical level MIP DEM capability to provide horizontal exchange of C2 information in MIP DEM format (Block 2 compliant) at Brigade and below level from the UK Tactical Communications System, BOWMAN.
GRB-Mercury	Provision of a rapidly deployable mobile broadband communications network capable of supporting NRF activities
GBR- CC2IWS	The CC2IWS node in UK will use MIP Block 2 to receive information from NATO using MIP Block 2. It will also be possible to receive information in other formats.
GBR – JCOP	CoJOP is the coalition deployment of our openJOP that delivers the Joint Operations Picture (JOP) on the (UK) Defence Information Infrastructure (DII).
GBR- ACTS	ACTS is the integration of applications (e.g. ICC and NIRIS) into a Service Orientated Architecture (SOA) to create an Air Component Command (ACC) toolset.
GBR- ADE	Test the integration, visualisation and dissemination of Air Defence (AD) and related sensor information to support NRF and related operations and develop enhanced capabilities for Air Defence systems to enable information to be used to support sensor integration and C3ISR information dissemination using standard NATO messaging and other protocols.
UNITED STATES	
USA-GCCS-A	IT and ID of GCCS-A which provides a Common Operational Picture (COP), Relevant Ground Picture (RGP) and C2PC Situational Awareness services during the scenario trials.
USA-TBMCS-UNITE	TBMCS: Use emerging internet technologies to enhance TBMCS operations and future Airspace Operations Management (JASMAD) in Coalition Air Operation Center with NATO ACCS, NATO ICC and NEC-CCIS. JASMAD: provide a single, joint, net-centric airspace management and dynamic deconfliction capability to coordinate near-real-time ACO planning and execution among the service components and coalition partners.
USA-COSMOS (3.14)	COSMOS will provide protected and role-based sharing using the command and control information exchange data model (C2IEDM) and the data exchange mechanism (DEM) of the Multi-lateral Interoperability Program (MIP).
USA-SIMEN (6.74)	Information Assurance (IA) monitoring for bandwidth-constrained environments and intermittently attached network enclaves
USA-GPRS (3.09)	Global Personnel Recovery System (GPRS) is an evolving, worldwide, over-the-horizon tracking, tagging, and locating two-way messaging system. Providing true worldwide, near-real-time communications and geo-location ability, GPRS is designed primarily for mobile users, providing force tracking and situational awareness for coalition combatants or other agency/first responders.
USA-JSF OMSE (5.08)	JSF's Off-board Mission Support Environment (OMSE) is a ground-based detailed mission planning system to support all aspects of mission preparation and post mission analysis. The intent is to demonstrate interoperability between the operational (NATO ACCS) and tactical levels (JSF OMS).Coalition Interoperability between operational and tactical level.
USA-JADOCS	JADOCS is a joint targeting and mission management software application used for targeting management and deconfliction processes, COP display using overlays, generate and distribute coordination measures, support base status management and data distribution, and support distributed coordination and collaboration between the EUCOM, NATO and UK nodes
USA-PROSAS	PROSAS includes a BUSTER unmanned aircraft system (UAS) for video and still image situation awareness; a precision fire software targeting solution; a Passive, Multistatic Network for stealthy maritime domain awareness; 'adLib' secure video and data management and distribution capability; a TRITON portal for displaying a user definable operational picture; possibly including a voice translator for nation-to-nation collaboration.
USA-RFW (2.37)	Digital dissemination of Missile Detection/Missile Warning (MD/MW) data to NATO partners over an INMARSAT broadcast to provide Situational Awareness, Force Warning and support to attack operations at the operational and tactical level.